

UNITED STATES DISTRICT COURT

for the
District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Device 1 and Device 2 as described in
Attachments A-1 and A-2

Casc No. 3:24-mc-1084 A-B

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Device 1 and Device 2 as described in Attachments A-1 and A-2 hereto,

located in the _____ District of _____ Oregon _____, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 1341, 1343, and 1349	Conspiracy to Devise or Intending to Devise Any Scheme or Artifice to Defraud by Means of Mail or Wire Communications

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ By phone

Applicant's signature

Special Agent Caryn Ackerman, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone at 2:40 pm (specify reliable electronic means).

Date: October 22, 2024

City and state: Portland, Oregon

Jolie A. Russo

Judge's signature

Hon. Jolie A. Russo, United States Magistrate Judge

Printed name and title

ATTACHMENT A-1

Device 1 is a black Apple iPhone with a white sticker on the back (hereinafter “**Device 1**”), which was found on the person of Biao **Lin** (hereinafter “**Lin**”) at the time of his arrest that occurred on October 4, 2024. **Device 1** is currently in the custody of the FBI Portland Division located at 9109 NE Cascades Blvd., Portland, Oregon, and identified and stored under FBI Case Number 196D-PD-3929089, Evidence Item 1B25.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT A-2

Device 2 is a lavender Apple iPhone (hereinafter “**Device 2**”), which was found on the person of Lin at the time of his arrest that occurred on October 4, 2024. **Device 2** is currently in the custody of the FBI Portland Division located at 9109 NE Cascades Blvd., Portland, Oregon, and identified and stored under FBI Case Number 196D-PD-3929089, Evidence Item 1B26.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on **Device 1** and **Device 2** (the **Devices**), as described in Attachments A-1 and A-2, that relate to violations of Title 18, United States Code, Sections 1341, 1343, and 1349, to-wit: engaging in a conspiracy to commit mail and wire fraud and involve **Biao Lin**, including:

- a. All records, documents, or materials, including correspondence, pertaining to the commission of, or conspiracy to commit, mail fraud and wire fraud, as those terms are defined in 18 U.S.C. §§ 1341, 1343, and 1349;
 - b. lists of victims and related identifying information;
 - c. any information related to co-conspirators and associates involved in the above violations (including names, addresses, phone numbers, or any other identifying information);
 - d. any information recording **Lin's** schedule or travel from **January 1, 2024**, to the present; and,
 - e. all bank records, checks, credit card bills, account information, and other financial records.
2. Evidence of user attribution showing who used or owned the **Devices** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or

stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Search Procedure

5. The examination of the **Devices** may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the **Devices** to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the **Devices** will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the **Devices** or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the **Devices** do not contain any data falling within the ambit of the warrant, the government will return the **Devices** to their owner within a reasonable period of time following the search and will seal any image of the **Devices**, absent further authorization from the Court.

9. If the **Devices** contain evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the **Devices** as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the **Devices** and/or the data contained therein.

10. The government will retain a forensic image of the **Devices** for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

DISTRICT OF OREGON, ss:

AFFIDAVIT OF CARYN ACKERMAN

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT FOR TWO PHONES

I, Caryn J. Ackerman, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since February 13, 2011. My current assignment is with the Portland Field Office, investigating financial crimes, public corruption, and federal civil rights violations. My training and experience include a law degree from the University of Oregon in 2007, successful completion of training at the FBI Academy in Quantico, Virginia, as well as subsequent participation in various trainings related to corruption, civil rights crimes, and money laundering.

2. I submit this affidavit in support of an application for a search warrant authorizing the search of Biao **LIN**'s cellular telephones (also referred to as **Device 1** and **Device 2**) as described in Attachments A-1 and A-2, for evidence, contraband, fruits, and instrumentalities, as described in Attachment B, of violations of Title 18, United States Code, Sections 1341, 1343, and 1349, which prohibit persons from conspiring to devise or intending to devise any scheme or artifice to defraud by means of mail or wire communications (the Target Offenses).

Identification of Devices to be Examined

3. **Device 1** is a black Apple iPhone with a white sticker on the back (hereinafter "**Device 1**"), which was found on the person of Biao **Lin** (hereinafter "**Lin**") at the time of his arrest that occurred on October 4, 2024. **Device 1** is currently in the custody of the FBI Portland Division located at 9109 NE Cascades Blvd., Portland, Oregon. **Device 1** is further identified and

stored under FBI Case Number 196D-PD-3929089, Evidence Item 1B25, and described in Attachment A-1.

4. **Device 2** is a lavender Apple iPhone (hereinafter “**Device 2**”), which was found on the person of **Lin** at the time of his arrest that occurred on October 4, 2024. **Device 2** is currently in the custody of the FBI Portland Division located at 9109 NE Cascades Blvd., Portland, Oregon. **Device 2** is further identified and stored under FBI Case Number 196D-PD-3929089, Evidence Item 1B26, and described in Attachment A-2.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. The statements contained in this affidavit are based upon the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience.

Applicable Law

6. Title 18, United States Code, Section 1341, prohibits a person, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, for the purpose of executing such scheme or artifice or attempting so to do, placing in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or depositing or causing to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or

PAGE 2 - AFFIDAVIT OF CARYN ACKERMAN

at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing.

7. Title 18, United States Code, Section 1343, prohibits a person, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, from transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

8. Title 18, United States Code, Section 1349, prohibits a person from conspiring or attempting to conspire to commit mail fraud, in violation of Title 18, United States Code, Section 1341, or wire fraud, in violation of Title 18, United States Code, Section 1343.

Statement of Probable Cause

9. On October 2, 2024, Adult Victim 1 (AV1) walked into the Portland Field Office of the FBI with her husband, Adult Victim 2 (AV2), and her son, to report she and her husband had been defrauded out of millions of dollars in gold bars at the direction of someone named “Michael Lewis” (hereinafter “Lewis”). Further, AV1 was still in contact with Lewis, and they were expected to provide additional gold at Lewis’s direction within the next few days. At the time of their reporting to the FBI on October 2, 2024, AV1 was 86 years old, and AV2 was 93 years old, and they had lost more than \$3 million, as a result of this scheme. AV1 and AV2 are residents of Portland, Oregon.

10. According to AV1, this all started on or about June 10, 2024, when AV1 tried to access her online accounts with Vanguard Group, where she had a trust account containing several million dollars, as well as an IRA with several millions of dollars as well. However,

instead of gaining access to her account, AV1 was notified her password was not working, and she was locked out of her account. AV1 was then called by someone purporting to be with the Vanguard fraud department and they told AV1 she had been locked out. In fact, AV1 was not contacted by someone from the Vanguard Group, but rather someone purporting to be who was instead a part of this fraud scheme.

11. AV1 was then called again by someone who identified himself as “Christopher Tyler” (hereinafter “Tyler”), also purportedly with the Vanguard fraud department. He was not. Tyler told AV1 her account had been hacked, that her Social Security number had been stolen and they had reported this to the Social Security Administration, that someone had tried to steal money from her Vanguard account, and that she had to take certain safety procedures to ensure her accounts would be safe. AV1 was then put in touch with “Anna Graves” (hereinafter “Graves”) at phone number (210) 460-7700, purportedly with the fraud section of the Social Security Administration; Graves in turn put AV1 in touch with “Michael Lewis” (hereinafter “Lewis”) at (410) 452-3406, who was purportedly with the Social Security Administration and was being assigned to her case. He was not actually with the Social Security Administration but rather another member of the fraud scheme. AV1 began communicating with Lewis with the goal of protecting her accounts from fraud.

12. On or about June 11, 2024, at Lewis’s direction, AV1 installed on her computer a software program called UltraViewer. According to UltraViewer’s website, it is a free remote desktop software, which allows a user “to remote control your client’s computer to support them like you’re sitting in front of the screen.” Lewis also asked for information about AV1’s personal life, including details about her banking institutions, grocery stores, and neighbors.

Lewis told AV1 he did not know the identities of the hackers putting AV1's accounts at risk, so AV1 must not tell anyone else or go on the Internet to seek information.

13. Lewis told AV1 that Vanguard only insured accounts up to a certain amount and since AV1 had more than that in her accounts, Lewis advised AV1 she had to move her money or else she would lose her money to these hackers. Lewis then directed AV1 to go to US Bank to buy gold bars as a way to safeguard her assets and that she then needed to transfer the gold to the U.S. Treasury for safekeeping, and after her accounts were deemed safe, they would transfer it back to her.

14. On or about June 24, 2024, AV1 used her US Bank account to initiate a wire transfer in the amount of \$466,043 USD to purchase gold bars, as directed by Lewis. Upon successful completion of this first purchase and conveyance of the gold bars, AV1 returned to US Bank to repeat the process and buy additional gold bars. However, US Bank refused to carry out the transfer. Lewis directed AV1 to open a new account at the Washington Federal Bank. The rest of the gold purchases were made via wire transfer from the Washington Federal account, which was funded by AV1's Vanguard accounts.

15. Throughout the weeks that followed, AV1 continued to purchase gold bars at the direction of Lewis.¹ These purchases were made with several different online gold vendors.

Lewis initiated the wire transfer with Washington Federal for each purchase, and Lewis would

¹ On or about July 4, 2024, AV1 was contacted by two agents with another federal investigative agency who advised she may be the victim of a fraud scheme. However, AV1 doubted whether the agents were really law enforcement officers. Lewis told AV1 he knew about the agents, and everything was under control, causing AV1 to continue making gold bar purchases at his direction. The FBI has confirmed the two agents who contacted AV1 were actual law enforcement agents with another agency.

advise AV1 to be available to verify the transaction with the bank. Soon thereafter, AV1 would receive an automated call from the bank asking her to verify the transaction.

16. Upon receipt of the gold bars via FedEx, AV1 took pictures of the gold bars and accompanying packing slips. The photos were sent to Lewis via text message, who would then contact her soon thereafter to repackage the gold bars on video. AV1 repackaged the gold bars at Lewis's direction, as he watched on video, wrapping them in Christmas or birthday paper.

17. Within a short amount of time, Lewis then recontacted AV1 to advise that a courier was on their way or imminently arriving to pick up the package. At this time, Lewis would provide AV1 with a password and tell her to ask the courier for the password before giving them the package. A courier would then arrive at her home, AV1 would ask the courier for the password, and then would hand the courier the package after receiving the password. Typically, Lewis remained on the phone with AV1 during the pickup.

18. AV1 said that the couriers were not from UPS, USPS, or FedEx, and they were dressed in normal attire. On several occasions, the courier was the same male individual, identified only as "Kevin." However, the last pick up before AV1 visited the FBI, the courier was an Asian woman accompanied by an Asian man in a car.

19. On each occasion, sometime after the package was conveyed, AV1 received from Lewis, via the Internet, what purported to be a U.S. Treasury check for the value of the gold bars. This process of purchase, repackaging, and pick up of the gold bars was repeated on multiple occasions, resulting in a total loss of over \$3,000,000 in gold.

20. On or about October 1, 2024, AV1 again made a purchase of gold bars via an online vendor in the amount of \$462,398, as directed by Lewis. Since the time of that purchase, AV1 revealed the situation with Lewis to her son and the FBI. AV1 expected to receive the gold

bars via FedEx with three to four days. Lewis continued to contact AV1 on October 2 and 3, 2024, but AV1 told Lewis her husband was in the hospital to limit interaction.

21. On or about October 3, 2024, AV1 was notified by FedEx that the package would be delivered to her residence in Portland, Oregon between 9:00AM and 1:00PM on Friday, October 4, 2024. AV1 believed Lewis was also likely to know when the package was scheduled for delivery, as she had observed him access her computer to view emails and other items. Lewis would then expect her to immediately repackage the gold bars on video. Further, AV1 expected that soon after repackaging the items, a courier would arrive at her house with a password to pick up the package. Agents advised AV1 to let Lewis know her husband was out of the hospital, and FBI Agents prepared a controlled pickup operation that took place on October 4, 2024.

22. On October 4, 2024, FBI Agents instructed AV1 to proceed with the process she had previously followed upon receipt of the gold via FedEx. AV1 took photos of the gold, which consisted of five one-kilogram gold bars and three smaller 100-gram gold bars, and sent them via text message to Lewis, then she waited for his direction to repackage them on video. FBI Agents also directed AV1's son to assist with preparing a decoy package, which would not actually contain gold bars, to be handed to the courier. A picture of the gold bars is below:

///

///

///



23. At approximately 11:25PM, Lewis advised AV1 two couriers² would be coming for pick up, and the couriers may not arrive until 2:30PM or 3:00PM. Lewis then proceeded to direct AV1 to package the gold in two separate boxes with one box containing two kilograms of gold and the other box containing 3.3 kilograms of gold. Lewis also directed AV1 to package the boxes in Christmas paper with the white side facing out. Lewis then directed AV1 to write her initials and the amounts on the boxes. AV1's son then proceeded to assist in preparing two decoy packages to match those previously packaged on video.

24. At approximately 3:45PM, Lewis called AV1 and stated the courier was outside, but upon opening her front door, AV1 found no one around. Soon thereafter, FBI Agents observed a Kia Soul with a Pennsylvania license plate parking near AV1's driveway, and then begin to proceed up the long driveway toward AV1 and AV2's residence. AV1 and AV2's residence is in Portland, Oregon. During this time, AV1 remained on the line with Lewis, who

² In later communications that followed, Lewis referred to only one courier.

conveyed the password was “Richard.” At approximately 3:50PM, the courier arrived at the door, and AV1 asked him for the password. The man, later identified as **Biao Lin** (hereinafter “**Lin**”), uttered the password “Richard,” and AV1 then handed him the two boxes. After **Lin** gained possession of the boxes and began to walk away from the house, FBI Agents moved in and placed him in custody.

25. As FBI Agents engaged with **Lin**, **Lin** refused to acknowledge any understanding of the English language. Agents began efforts to obtain the assistance of a Mandarin interpreter to communicate with **Lin**.

26. With the assistance of a Mandarin interpreter translating by phone, Agents provided **Lin** his constitutional Miranda warnings, and **Lin** acknowledged understanding his rights and agreed to speak with the Agents. **Lin** explained he was randomly approached by an unknown Asian man about a week ago in a New York City library. **Lin** said was offered \$200 to fly somewhere to pick something up, and he agreed. The man gave **Lin** a phone, which was not password protected. **Lin** was told he would get instructions on that phone.

27. **Lin** stated he flew into Spokane, Washington yesterday, October 3, 2024, and he made no other stops except to drive directly to Portland. **Lin** said the person who gave him directions on the phone spoke Mandarin with a western accent. **Lin** stated he was told to pick up a package, but he was not told any passwords. **Lin** was supposed to get additional information via phone after picking up the package, but instead he was arrested. **Lin** denied knowing what he was picking up. He advised he had only his suitcase and backpack in the car, and he said the car did not contain any drugs, money, weapons, or gold.

28. On **Lin**’s person, Agents found **Device 1** and **Device 2**, as well as what appeared to be part of a Delta boarding pass for a flight from Atlanta to Spokane for October 3. Concealed

in **Lin**'s jacket was \$5,000 in the form of 50 crisp one-hundred-dollar bills, and Agents found \$1,394 in cash in his wallet. **Lin** advised he had not yet been paid for making this pick up, as he was supposed to be paid afterward. According to **Lin**, he had to pay for the car rental and flight on his own.

29. I know from this investigation that **Lin** has admitted **Device 1** was given to him for the purpose of communicating with at least one other member of the conspiracy to receive instructions to pick up a package at AV1's residence. **Lin** also explained he would have received further instruction via **Device 1** for handling of the package had he not been arrested. Accordingly, I believe there is probable cause to believe there are communications and other evidence of the Target Offenses, as outlined in Attachment B, within **Device 1**.

30. **Lin** further advised agents **Device 2** was his personal cell phone. Based on my training and experience, I know people tend to use their personal devices for a variety of travel-related activities, such as making purchases and travel plans, communicating with family and friends about their whereabouts and status of travel, using ride service applications, and for mapping directions while driving. Based on my familiarity with other investigations involving gold couriers, I know couriers travel throughout the country to pick up gold from victims and deliver it to co-conspirators. Similarly, in this case, I believe **Lin** traveled via plane from Atlanta to Spokane, then rented a car and drove from Spokane to AV1's residence in Portland. Because **Device 2** was **Lin**'s personal cell phone, and it was on his person at the time of his arrest, I believe that despite the presence of **Device 1**, it is likely **Lin** continued to use **Device 2** to carry out daily activities and activities related to his travel. Consequently, I believe information related to **Lin**'s past travel and movements will be found on **Device 2** and could reveal additional victims of the conspiracy and the locations of co-conspirators. Therefore, I have probable cause

to believe evidence of the Target Offenses, as outlined in Attachment B, will also be found on **Device 2.**

Search and Seizure of Digital Data

31. This application seeks permission to search for particular items, described in Attachment B, in whatever form those items may be found. One form in which that evidence will likely be found is as data stored on a digital device, including a cell phone. Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Fed. R. Crim. P. 41(e)(2)(B).

32. Specifically, this application seeks permission to search for, seize, and examine:

a. All records, documents, or materials, including correspondence, pertaining to the commission of, or conspiracy to commit mail fraud and wire fraud, as those terms are defined in 18 U.S.C. §§ 1341, 1343, 1349;

b. Evidence of Internet usage for the commission of, or conspiracy to commit, mail fraud and wire fraud as defined in 18 U.S.C. § 1341, 1343, 1349, including dates and times of usage; IP addresses; and screennames, usernames, and passwords used to access the Internet or any accounts via the Internet;

c. Communications, including emails, chats, bulletin board posts, and comments, relating to the commission of, or conspiracy to commit, mail fraud and wire fraud; and

d. “Records,” “items,” “documents,” and “materials” include all of the foregoing items in whatever form and by whatever means they may have been created or

///

stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

33. Based on my training and experience and the knowledge obtained from other law enforcement officers, I know criminals involved in fraud crimes often try to conceal their methods of communication and their communication devices from law enforcement in order to use these devices to conduct their criminal activities without being caught. One such method of concealing communication methods and devices is to use multiple different communication devices, often changing which one is used. Based on my training and experience and the circumstances described herein, I believe **LIN** used **Device 1** and **Device 2** to communicate and conduct illegal activity related to the Target Offenses and that specific evidence, fruits, or instrumentalities of such illegal fraudulent activity will be found on the Phones.

34. In addition to the facts listed previously, I believe the facts and circumstances establish probable cause that the electronically stored information described in Attachment B is located on **Device 1** and **Device 2**, as described in Attachment A.

35. The Phones are currently in the lawful possession of the FBI Portland Division located at 9109 NE Cascades Blvd, Portland, Oregon. **Device 1** and **Device 2** were seized by FBI Special Agents during **LIN**'s arrest. In my training and experience, I know that the Phones have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as when the Phones first came into the possession of the FBI.

36. Based on my training and experience, a wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers,

enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; recording, storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet, including the use of apps. Wireless telephones may also include a global positioning system (“GPS”) technology for determining the location of the device.

37. Based on my training, experience, and research, I know that the Phone has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, and GPS navigation device. In my training and experience, examining data stored on wireless telephones can uncover, among other things, evidence that reveals or suggests who possessed or used the phone, how the phone was used, and the purpose of its use.

38. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrant but also forensic evidence that establishes how the Phones were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the Phones because, based on my knowledge, training, and experience, I know:

a. Phones can store information for long periods of time, including

information viewed via the Internet. Files or remnants of files can be recovered with

forensic tools months or even years after they have been downloaded onto a phone, deleted, or viewed via the Internet. Electronic files downloaded to a phone can be stored for years at little or no cost. When a person “deletes” a file, the data contained in the file does not actually disappear, rather that data remains on the phone until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the phone that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the operating system may also keep a record of deleted data.

b. Wholly apart from user-generated files, the Phones may contain electronic evidence of how it has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, and file system data structures.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

d. Data on the Phones can provide evidence of a file that was once on the Phones but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Systems can leave traces of information on the Phone that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the Phones that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, including SD cards or other flash media, and the times the Phones were in use. File

systems can record information about the dates files were created and the sequence in which they were created.

e. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

f. A person with appropriate familiarity with how the Phones work may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the Phone was used, the purpose of its use, who used it, and when.

g. The process of identifying the electronically stored information necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on the Phones is evidence may depend on other information stored on the Phones and the application of knowledge about how Phones function. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

h. Further, in order to find evidence of how the Phones were used, the purpose of their use, who used them, and when, the examiner may have to establish that a particular thing is not present on the Phones.

39. I know that when an individual uses a wireless telephone to commit a crime such as to communicate about or arrange mail or wire fraud, the phone will generally serve both as an instrumentality for committing the crime and as a storage medium for evidence of the crime. From my training and experience, I believe that a phone used to commit a crime of this type may

contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

40. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Phones consistent with the warrant. The examination may require authorities to employ techniques, including imaging the Phones and computer-assisted scans and searches of the entire Phones that might expose many parts of the devices to human inspection in order to determine whether it constitutes evidence as described by the warrant.

41. The initial examination of the Phones will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

42. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Phones or images do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

43. If an examination is conducted, and it is determined that the Phones do not contain any data falling within the ambit of the warrant, the government will return the Phones to their owner within a reasonable period of time following the search and will seal any image of the Phones, absent further authorization from the Court.

44. If the Phones contain evidence, fruits, contraband, or are an instrumentality of the crime, the government may retain the Phones as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Phones and/or the data contained therein.

45. The government will retain a forensic image of the Phones for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

46. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

47. Based on the foregoing information, I respectfully submit that there is probable cause to believe that the phones described in Attachments A-1 and A-2 (**Devices 1 and 2**) contain evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1341, 1343, and 1349, as set forth herein and in Attachment B. I therefore respectfully request

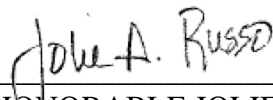
PAGE 17 - AFFIDAVIT OF CARYN ACKERMAN

that the Court issue a warrant authorizing a search of the cell phones (**Devices 1 and 2**) described in Attachments A-1 and A-2 for the items listed in Attachment B and the seizure and examination of any such items found.

48. This affidavit, the accompanying application, and the requested search warrant were reviewed by Assistant United States Attorney (AUSA) Scott Kerin prior to being submitted to the Court. AUSA Kerin informed me that in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

By phone pursuant to Fed. R. Crim. P. 4.1
CARYN J. ACKERMAN
Special Agent
Federal Bureau of Investigation

Sworn via telephone pursuant to Fed. R. Crim. P. 4.1 at 2:40 pm on October
22, 2024.



HONORABLE JOLIE A. RUSSO
United States Magistrate Judge